

REMARKS/ARGUMENTS

The present application provides a method for creating, storing and reading a new certificate type for certification of keys. In the new certificate type, several certificates, containing redundant data fields, are collated to form one certificate and repetition of redundant information on the certificates is eliminated by use of a group certificate. The group certificate is used where several keys are to be issued at the same time for the same user by the same certification instance. By means of the group certificate, repetition of all redundant data elements are eliminated and all data elements for a set of several keys subject to certification are grouped into one certificate. This substantially reduces the memory requirement, and handling of the certificates is simplified for the communication partners. A further embodiment of the new certificate type is the basic and supplementary certificate combination. This form of certification is used where certificates are issued at different times for the same user by the same certification body. The memory requirement is consequently somewhat more than for group certificates, but greater flexibility is gained in use of the keys.

Claim Rejections Under 35 USC 103

A. Claims 1 to 12 were rejected under 35 USC 103(a) as being unpatentable over VeriSign "Certificate Practice Statement", version 1.2, in view of Stallings "Cryptography and Network Security", 2nd Edition, and Karlton "Proposal to Add Attribute Certificates to TLS 3.1".

The Examiner points out that VeriSign does not teach the use of a supplementary certificate for the issuance of additional keys and relies on the teaching of the Karlton reference to provide the missing teaching. However, Karlton clearly states that attribute cert shall have no associated key pair. Therefore, the Karlton teaching specifically excludes its attribute certificates for applicant's purposes. Therefore, there not only is a lack of teaching applicant's invention in the proposed combination, but a specific exclusion of any such teaching of supplementary certificates for the purposes proposed by applicants. Without the issuance of further keys in the supplementary certificate, the advantages in accordance with the applicant's invention are not obtained. Further, the reasons given for justification to making the combination, in absence of a clear prior art showing of applicant's invention, is more an indication of the unobviousness of that invention than it is of its obviousness.

The Examiner also points out that VeriSign does not disclose a certificate designed to carry a plurality of keys and discusses the Stallings article in this connection. However, the Examiner points out that he found nothing in the Stallings article that mentions a group certificate containing multiple keys. Therefore there is no teaching in the combination for a group certificate designed to carry multiple keys. Again, the reasoning behind the Examiner's reasoning for making the combination in absence of the existence of applicant's invention is more an indication of the non-obviousness of what applicant has done than an indication of its obviousness.

B. Claims 13 to 18 were rejected under 35 USC 103(a) in view of the combination cited in A further in view of the Deo, U.S. patent #5,721,781; and

C. Claims 19 to 25 were rejected over the prior art cited against claims 1 to 7 in A further in view of “JAVA XZ509 Certificates and Certificate Revocation Lists.” The arguments presented in A with respect to claims 1 to 7 apply equally well to the Examiner’s position with respect to rejection of claims 18 to 25 in B and C.

The claims in the application are all allowable for the reasons given above. All independent claims are limited either to sequential or supplementary certificates, each for a different key or a group certificate for multiple keys both which, as pointed out above, are not disclosed by the combination. The dependent claims further distinguish over the prior art in that they cite details of the contents of certificates for multiple keys and sequential supplementary certificates containing keys.

Claim Rejections Under 35 USC 112

Claims 1, 4 and 8 have been amended to eliminate the issue of the lack of antecedent basis for terms used in those claims.

New Drawings

A new set of drawings accompanies this amendment. Please substitute these formal drawings for the ones that were originally submitted.

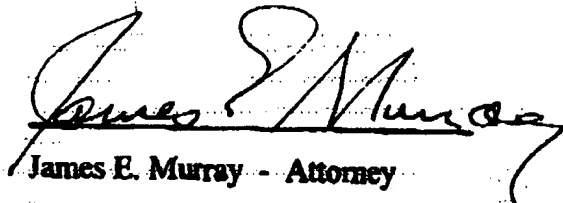
GE999008

Specification

A new title has been submitted. The mentioned trademarks are adequately protected by the present description in the application. All are accompanied by a generic term and an indication of their ownership.

For the above reasons, the application is in condition for allowance and it is therefore respectfully requested that it be reconsidered, allowed to passed to issue.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "James E. Murray", is written over a horizontal line.

James E. Murray - Attorney

Reg. No.: 20,915

Telephone No.: (845) 462-4763